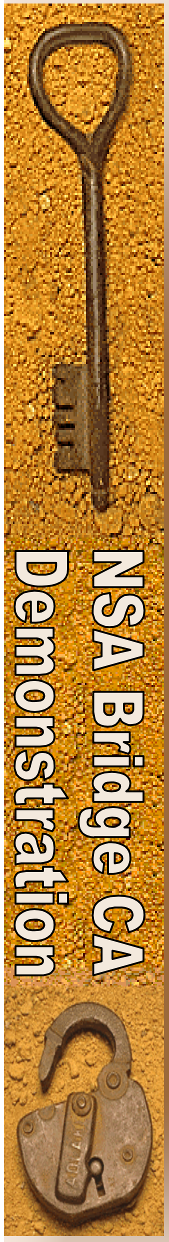
National Security Agency

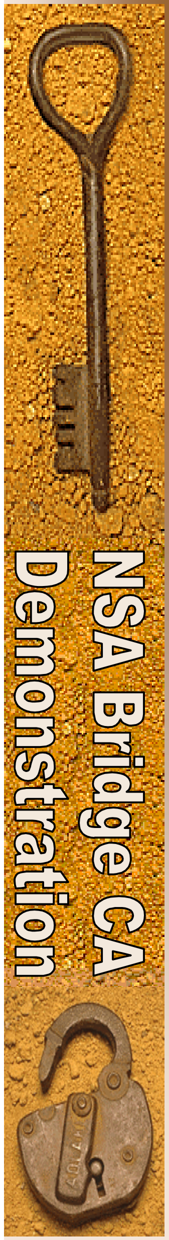


NSA Bridge CA Demonstration

Bridge Certification Authority Technology Demonstration Phase 2

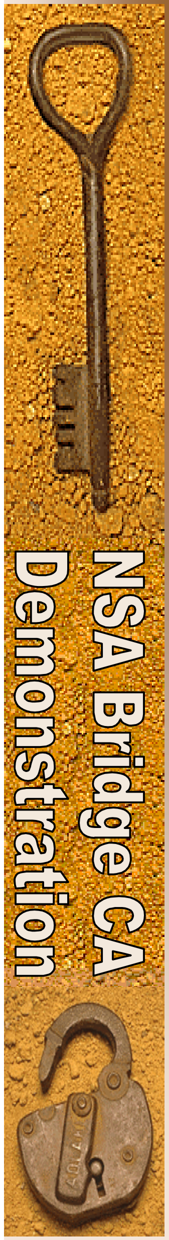
Briefing to Federal PKI Technical Working Group

2 August 2001
Dave Fillingham, NSA
dwfilli@missi.ncsc.mil



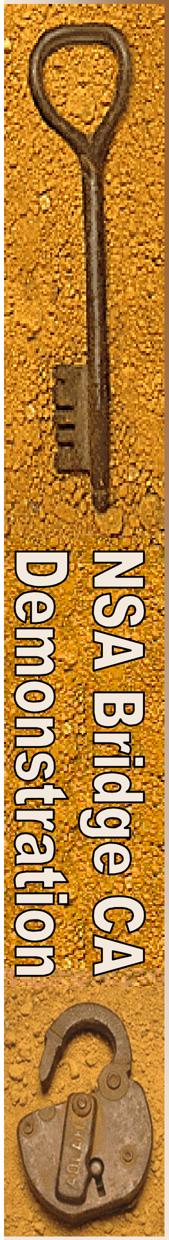
Overview

- What we'll be talking about today
- What's new, what's old?
- Bridge CA background
- Strategy and tactics



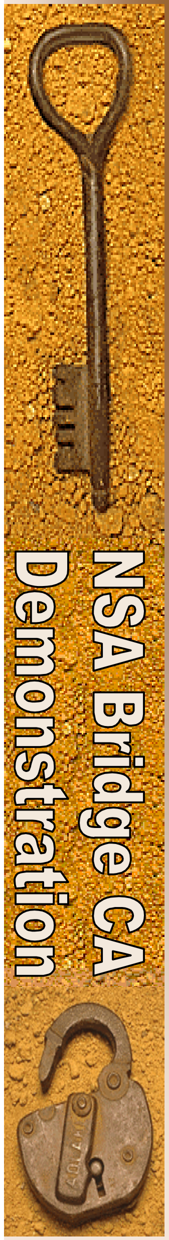
Who You’ll be Hearing From

- Dave Lemire - A&N
  - System Overview
- Peter Hesse, Cygnacom/Entrust
- John Pawling, Getronics
- Al Ferguson, SPYRUS
- Rachel Shea, Baltimore
- Pete Peterson, Entegrity
- Dave Lemire - A&N
  - Lessons Learned
- Discussion



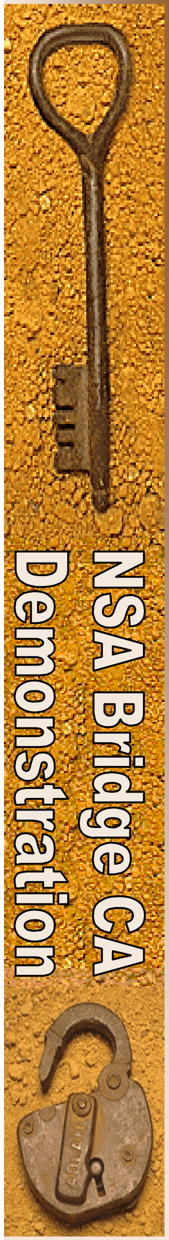
FPKI Problem

- Provide PKI Interoperability Throughout Federal Government
  - Single Federal Root Not Acceptable
  - Numerous PKIs Already In Place / Being Fielded
- Need to Establish Trust Paths
- Need to Ensure Certificate / CRL Availability
- Need “Bottom Up” Solution



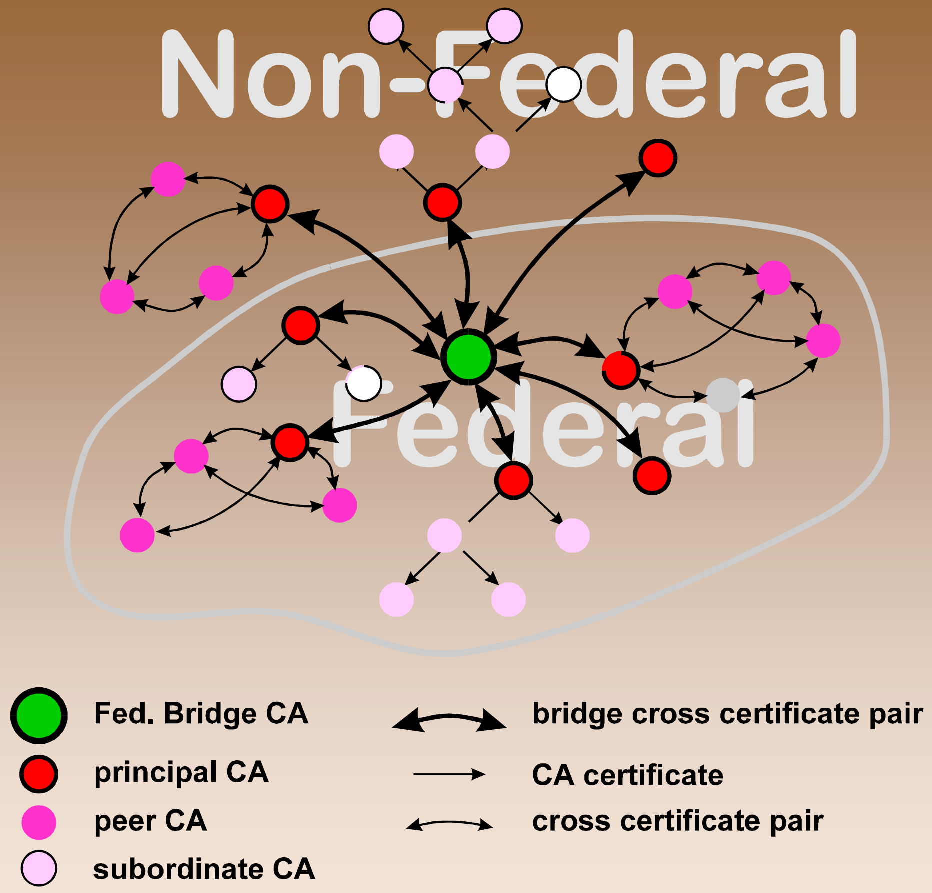
FPKI Proposal

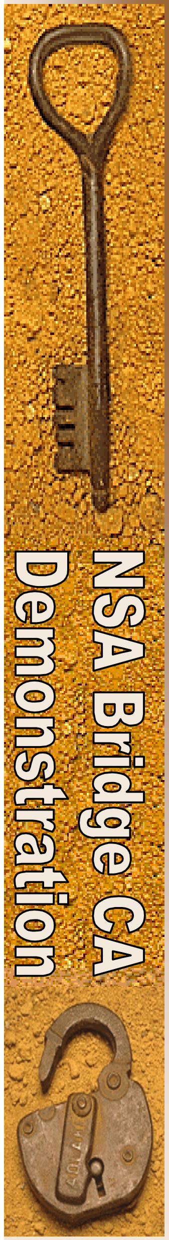
- Build the nexus to connect the pieces
- Three key elements:
  - Federal “Bridge” CA (BCA)
    - **Not a Root!**
    - Cross certifies with Principal CAs (PCAs) in Different Domains
  - Federal Policy Authority (PA)
  - Bridge CA Repository
    - for CA certificates and status



NSA Bridge CA Demonstration

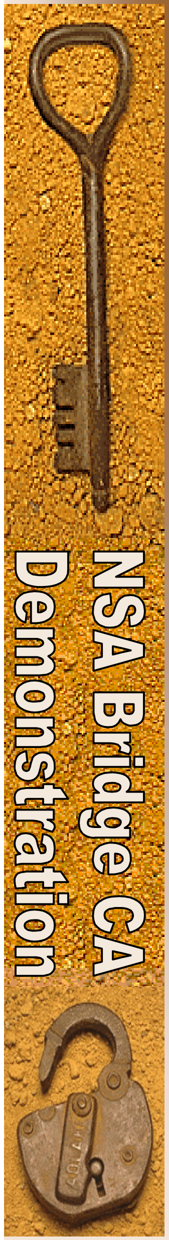
FPKI Architecture





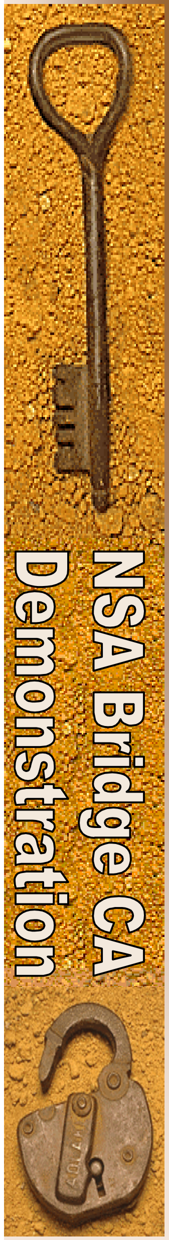
The BCA Demo - Problem Overview

- Multiple PKIs of Interest to US Department of Defense
  - DoD PKI
  - DoD Network Security Manager / Defense Message System / FORTEZZA PKI
    - Part of Future Key Management Infrastructure (KMI)
  - Federal Bridge Certification Authority PKI
  - PKIs Used by US Allies
  - Commercial Products Used by Vendors and Contractors
- Many PK-aware applications will not work outside their own PKI
- Many commercial client products have limitations which make using the BCA difficult



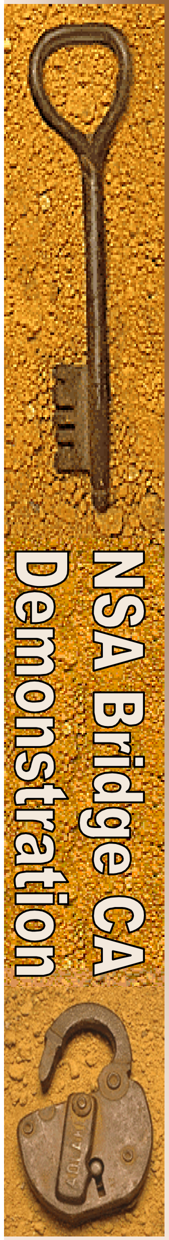
BCA Demonstration Objectives and Strategies

- Further DoD / Federal PKI Interoperability
  - **Break down "psychological" resistance to the concept by proving technology was doable**
    - Demonstrations to vendor community to increase their awareness of capabilities
    - Demonstrations to government community to increase market demand
  - **Reduce vendor investment requirements to BCA enable clients**
    - Freeware software and documentation
    - Free access to testing data and facilities



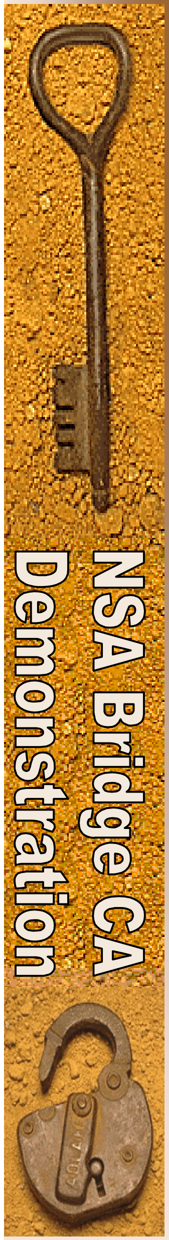
BCA Demonstration Objectives and Strategies

- **Make BCA enabled software commercially available for government purchase**
  - Collaborative development enabled rapid cross-vendor agreement on technical solutions, standards interpretation
  - Sometimes direct tasking to participants to make results of BCA effort available commercially
- **Discover and eliminate technical barriers to interoperation in commercial products**
  - Problems discovered and eliminated during development
  - Make “lessons learned” available to non-participants via study reports



BCA Demonstration Objectives and Strategies

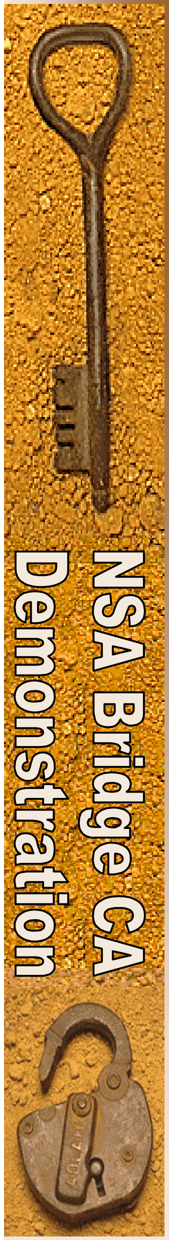
- Show that access control technologies can be built on an interoperable authentication foundation to provide powerful information management tools



The 1999 Phase I Demo

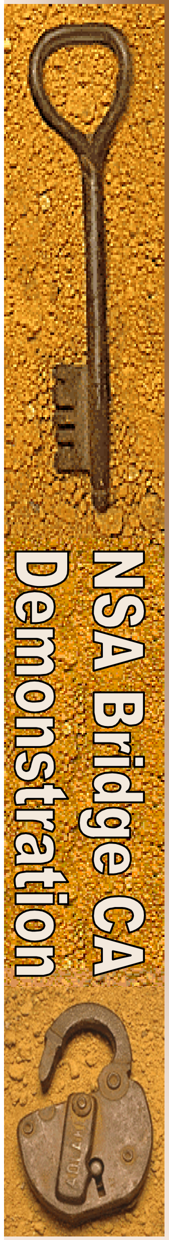
3 PKIs + Bridge / 4 Vendors

- Signed E-Mail
- Single Signature Algorithm (RSA)
- Single Hash Algorithm (MD5)



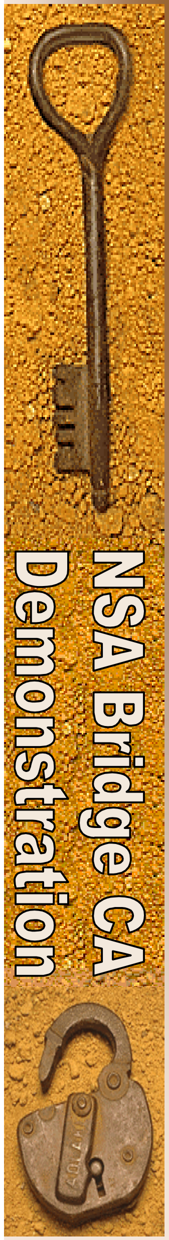
What’s New?

- Phase 2 Demonstration Has
  - **6** PKIs + Bridge / **6** Vendors
  - Signed, **Encrypted, Labeled** E-Mail
  - **Certificate Policies**
  - **Name Constraints**
  - **Secure Web Server**
    - **SSL w/Client Certificate Verification in BCA Environment**



What's New?

- Phase 2 Demonstration Has (Cont'd):
  - **Multiple** Signature Algorithms (RSA, **DSA**)
  - **Multiple** Hash Algorithms (MD5, **SHA-1**)
  - **Content Encryption Algorithm (3DES)**
  - **Key Management Algorithm (RSA)**
  - **Access Control for E-Mail and Web Using**
    - **Security Policy Information File**
    - **Attribute Certificates**



The Players

Government Lead: NSA

Getronics

Entrust®
Securing the Internet

BALTIMORE™

CYGNACOM SOLUTIONS
an Entrust company

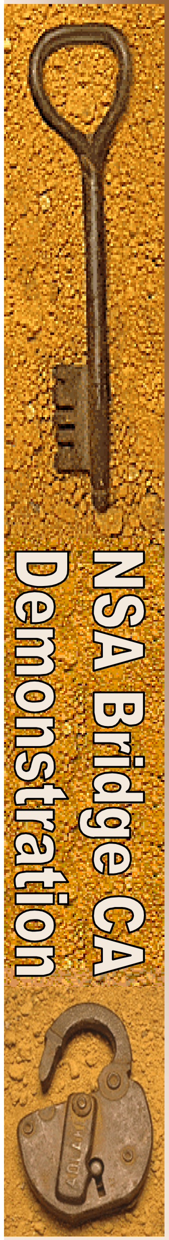
SPYRUS

ENTEGRITY Solutions®

A&N Associates, Inc.

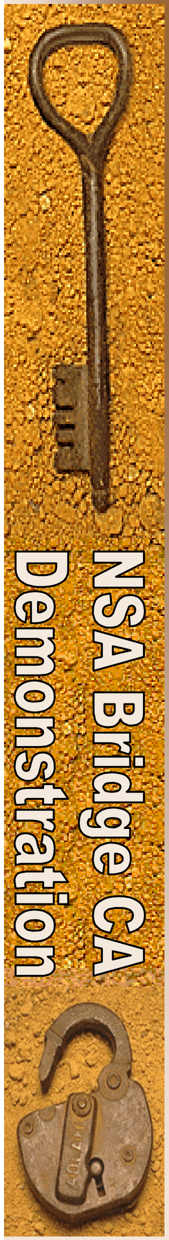
SETECS
Secure Transactions and Electronic Commerce Systems

MOTOROLA



Sun Microsystems

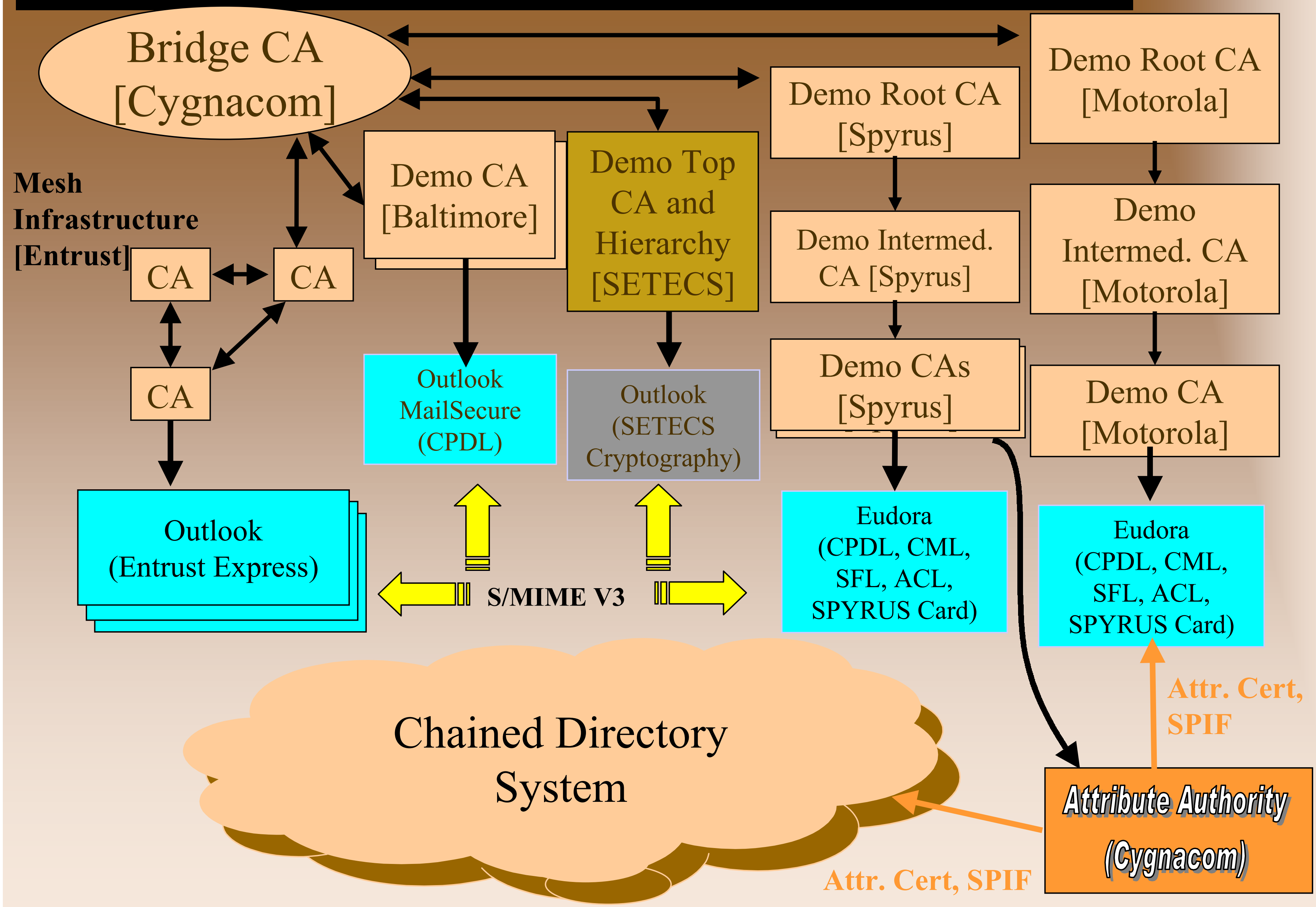
- Java[TM] 2 Platform, Standard Edition, v 1.4 will include certification path development and validation features
- Sun successfully completed interoperability testing between a prerelease version of this software and the DoD Bridge CA Technology Demonstration
- A beta version of this code is available from http://java.sun.com
- For more information, contact: steve.hanna@sun.com

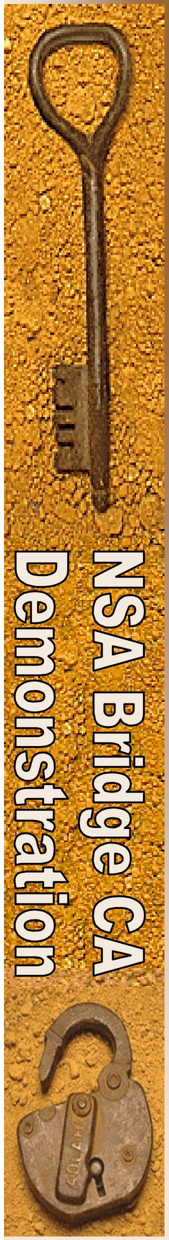


Client Limitations Contributing to PKI Stovepipes

Issue	Demo Solution
Certificate Path Development	Certificate Path Development Library
Certificate Path Processing	Certificate Management Library
Algorithms	Algorithm Agility
Secure Message Protocol	S/MIME Freeware Library
Directory Access	Chained Commercial Directories Border Directory

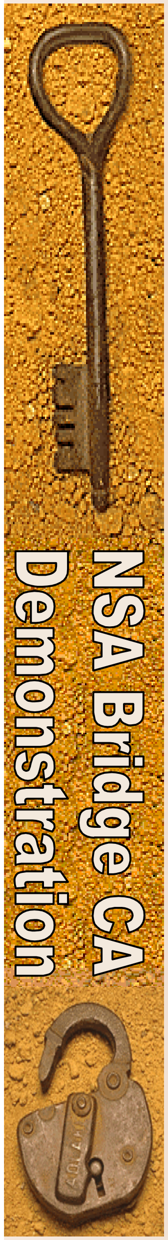
BCA Phase 2 Demonstration Architecture Summary


Bridge CA [Cygnacom]
Mesh Infrastructure [Entrust]
CA
CA
CA
Demo CA [Baltimore]
Demo Top CA and Hierarchy [SETECS]
Demo Root CA [Spyrus]
Demo Root CA [Motorola]
Demo Intermed. CA [Spyrus]
Demo Intermed. CA [Motorola]
Demo CAs [Spyrus]
Demo CA [Motorola]
Outlook MailSecure (CPDL)
Outlook (SETECS Cryptography)
Outlook (Entrust Express)
S/MIME V3
Eudora (CPDL, CML, SFL, ACL, SPYRUS Card)
Eudora (CPDL, CML, SFL, ACL, SPYRUS Card)
Attr. Cert, SPIF
Chained Directory System
Attr. Cert, SPIF
Attribute Authority (Cygnacom)

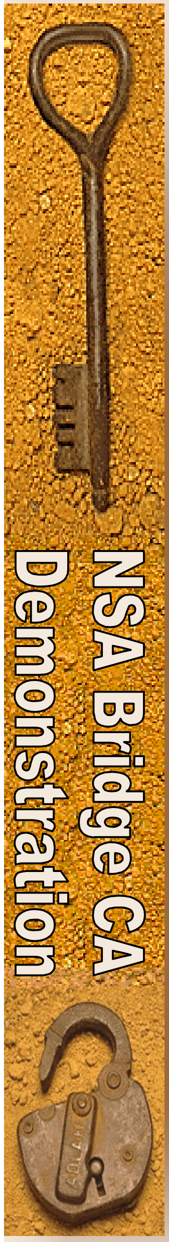


Available Software Modules

Module	Developer
Certificate Path Development Library (CPDL) http://www.cygnacom.com/products/index.htm	CygnaCom
Certificate Management Library (CML) http://www.getronicsgov.com/hot/cml_home.htm	Getronics
S/MIME Freeware Library (SFL) http://www.getronicsgov.com/hot/sfl_home.htm	Getronics
Access Control Library (ACL) http://www.getronicsgov.com/hot/acl_home.htm	Getronics
Entrust Toolkit http://www.entrust.com/developer/software/index.cfm	Entrust



On to the technical briefings…



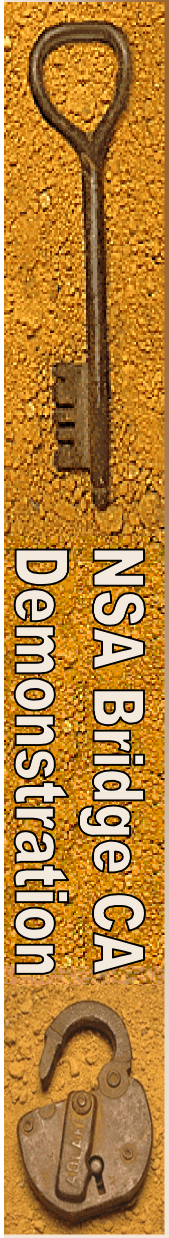
NSA Bridge CA Demonstration

National Security Agency

Wrap-Up and Summary

Briefing to Federal PKI Technical Working Group

2 August 2001
Dave Fillingham, NSA
dwfilli@missi.ncsc.mil

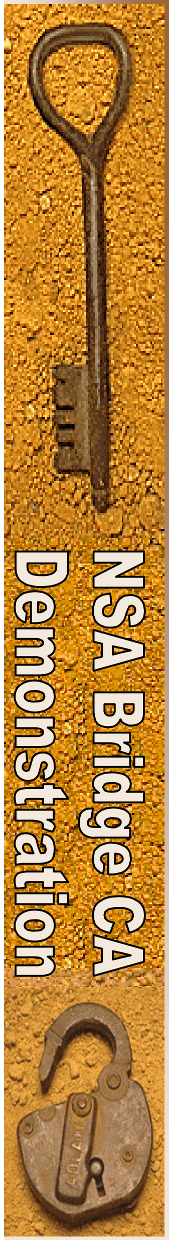


What Are We Getting?

- Promote Cross-Federal security interoperation
- Demonstrates a Model for Allied Interoperation
- Provide an Option Besides Trust Lists
- Promotes Development of Commercial Products that function in BCA Environment
- Complete Interoperability Solution
- Software Libraries Available for Integration Into Commercial Products
  - S/MIME
  - Access Control
  - Certification Path Development
  - Certification Path Validation

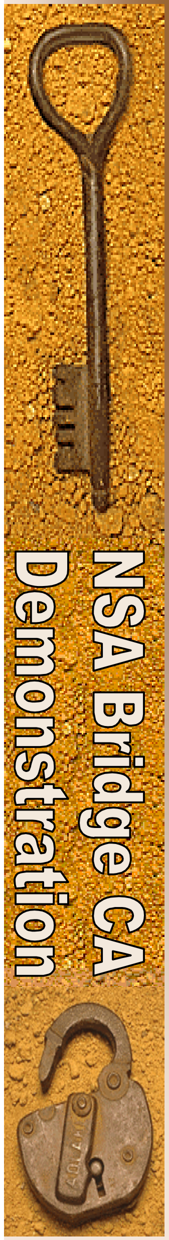
Summary

- Bridge CA seems a good approach to achieve interoperability among “equal” public key infrastructures
- Border Directory concept provides “certificate path” interoperability
- Application limitations are a problem - but “BCA capable” applications are available



Summary

- Bridge CA demonstration attempts to prove technology, and accelerate application developments
- BCA demonstration Phase I proved concept using RSA and digital signatures, and border directories
- BCA demonstration Phase II includes encryption, attribute certificates, multiple signature algorithms, and web security



Would you like to see the demo?

- Cygnacom/McLean
  - Date: 16 August 2001
  - Times: 0900, 1300
  - Duration: about 31/2 hours

- Getronics Government Solutions, Annapolis Junction
  - Date: 17 August 2001
  - Time: 0900
  - Duration: about 31/2 hours

- Directions, sign-up sheet available here